NEWS FROM U.S. SENATOR SHELDON WHITEHOUSE

FOR IMMEDIATE RELEASE
July 15, 2014

Contact: Seth Larson
(202) 228-6291 (press office)

Opening Statement of Sheldon Whitehouse
Chairman, Judiciary Subcommittee on Crime and Terrorism
Hearing on: "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

As Prepared for Delivery

Washington, DC – Welcome to today's hearing entitled "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks."

Today, this Subcommittee will hear testimony about botnets and the threat they pose to our economy, our privacy, and our national security. A botnet is simply a network of computers connected over the internet that can be instructed to carry out specific tasks – typically without the owners of those computers knowing it.

Botnets have existed in various forms for well over a decade, but they are now recognized as the weapon of choice for cyber criminals. It is easy to see why: A botnet can increase the computing resources at a hacker's disposal exponentially, while helping conceal the hacker's identity. A cyber criminal with access to a large botnet can command a virtual army of millions – most of whom have no idea they have been conscripted.

Botnets enable criminals to steal individuals' personal and financial information, plunder bank accounts, and commit identify theft on a massive scale. For years, botnets have sent most of the spam we all receive; the largest botnets are capable of sending billions of spam messages per day. Botnets are used to launch distributed denial of service (or DDoS) attacks, which can shut down websites by overwhelming them with traffic – a constant danger for businesses in every sector of our economy. The only limit to the malicious purposes for which botnets can be used may be the imaginations of the criminals who control them – and when a hacker runs out of uses for a botnet, he can simply sell it to another criminal organization to use for an entirely new purpose.

Let's be clear: the threat from botnets is not just to our wallets. Botnets are effective weapons not merely for those who want to steal from us, but also for those who wish to do us far more serious harm. Experts have long feared the next 9/11 may be a cyber attack. If that is the case, it is likely that a botnet will be involved. Simply put, botnets threaten the integrity of our computer networks, our personal privacy, and our national security.

In recent years, the government and the private sector have launched aggressive enforcement actions to disrupt and disable individual botnets.

The techniques used to go after botnets are as varied as the botnets themselves. Many of these enforcement actions use the court system to obtain injunctions and restraining orders, utilizing innovative legal theories combining statutory claims under the Computer Fraud and Abuse Act and other laws with ancient common-law claims like trespass to chattels.

In 2011, the government obtained – for the first time – a court order that allowed it to seize control of a botnet using a substitute command and control server. As a result, the FBI launched a successful takedown of the Coreflood botnet, freeing 90% of the computers it had infected in the United States.

Microsoft, working with law enforcement, has obtained several civil restraining orders to disrupt and, in some cases, take down individual botnets, including the Citadel botnet, which was responsible for stealing hundreds of millions of dollars from bank accounts. And earlier this year, the Justice Department and the FBI, working with the private sector and law enforcement agencies around the world, obtained a restraining order allowing them to take over the Gameover Zeus botnet. This action was particularly challenging, because the botnet relied on a decentralized command structure that was designed to thwart efforts to stop it.

Each of our witnesses today has played a role in efforts to stop botnets. I look forward to learning more about these and other enforcement actions and the lessons that have been learned from them. We must recognize that enforcement actions are just one part of the answer, so I am interested in hearing about how we can better inform computer users of the dangers of botnets and what other steps we can take to address this threat.

My hope is that this hearing starts a conversation among those dealing day-to-day with the botnet threat and those of us in Congress who are deeply concerned about that threat. Congress, of course, cannot and should not dictate tactics for fighting botnets; that must be driven by the expertise of those on the front lines of the fight. But Congress does have an important role to make sure that there is a solid legal foundation for enforcement actions against botnets and clear standards governing when they can occur. We must also ensure that botnet takedowns and other actions are carried out in a way that protects consumers' privacy, while recognizing that botnets themselves represent one of the greatest privacy threats computer users face today. And we must make sure our laws respond to a threat that is constantly evolving, and encourage, rather than stifle, innovative efforts to disrupt cyber criminal networks.

I look forward to starting this conversation today and to continuing it in the months ahead. I thank my distinguished Ranking Member for being such a terrific colleague on these cyber issues. I thank you all for participating in this hearing and for your efforts to protect Americans from this dangerous threat.

###